A METHOD FOR PROTECTING A PORTABLE CARD

[0001] BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The invention relates to a method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key through statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power consumption data, electromagnetic radiation and the like. The card is provided with at least a shift register having a linear and a non-linear feedback function for creating cryptographic algorithms. The method comprises loading data to be processed and a secret key in the shift register of the card.

[0004] 2. Description of the Prior Art

[0005] Using a secret key to process input information and/or to produce output information is generally known in the event of cryptographic devices. Using feedback shift registers is also generally known for creating cryptographic algorithms.

[0006] In this connection, data to be consecutively processed and a secret key are loaded into one or more shift registers. Here, the sequence of loading data and the key is random.

[0007] Subsequently, the output of the shift register and possibly the shift-register contents are applied, using linear and/or non-linear-feedback, to determine the output of the entire algorithm. The input of the shift register then, apart from the data and the key, also consists of a linear and a non-linear combination of the shift-register contents.

[0008] Such shift registers are generally applied in the event of portable cards, such as chip cards, calling cards, smart-card products and the like.

[0009] Since the secret key is not known to unauthorized third parties, it is basically impossible to derive either the input or the key from the output of the algorithm.

[0010] Now it has become apparent, however, that for chip cards and the like it is possible, in the event of computations, to derive the secret key used from a statistical analysis of the power consumption of the card. Such methods are known as "Differential Power Analysis" (= DPA) and are described in the Internet publication DPA Technical Information: "Introduction to Differential Power Analysis and Related Attacks" by P. Kocher et al., Cryptography Research, San Francisco, 1998.

[0011] Such methods are based on the fact that, in practice, with cryptographic operations, information is

leaking away to the outside world in the form of power-consumption data, electromagnetic radiation and the like.

[0012] Thus, logical microprocessor units show regular transistor-switching patterns which externally (i.e., outside the microprocessor) noticeably produce electrical behaviour.

[0013] In this manner, it is possible to identify macro characteristics, such as microprocessor activity, by recording the power consumption and deriving information on the secret key used by way of statistical analysis of the data thus obtained.

[0014] SUMMARY OF THE INVENTION

[0015] The invention now overcomes this drawback in the art and provides a portable card which is resistant to such analyses and therefore provides a card which is safe to use.

[0016] The method according to the invention is characterized in that an algorithm is applied to the card which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key by way of statistical analysis of those values. Advantageously, after loading the key into the shift register, the shift register is subsequently clocked on, during a specific period of time, several times, at least making use of the linear feedback function.

[0017] A suitable alternative according to the invention is loading only the key into the shift register in the event of a fixed content of the shift register.

[0018] In a first advantageous embodiment of the invention, there is first loaded the key, subsequently clocking on is performed, after which the data is loaded.

[0019] In another advantageous embodiment of the invention, the key is first loaded, subsequently the data is loaded into the shift register, making exclusive use of the linear feedback function and subsequently the clocking on is performed.

[0020] In yet another advantageous embodiment of the invention, the data is first loaded, subsequently the key is loaded, making exclusive use of the linear feedback function, whereafter clocking on is performed.

[0021] BRIEF DESCRIPTION OF THE DRAWINGS

[0022] The invention will now be further explained with reference to the drawing and the description by way of non-limiting examples.

[0023] FIG. 1 schematically shows a typical shift register as applied with a portable card, such as a chip card and the like.

[0024] FIG. 2 schematically shows an advantageous solution according to the invention, and

[0025] FIG. 3 schematically shows another advantageous solution according to the invention.

[0026] DETAILED DESCRIPTION

[0027] Referring now to FIG. 1, there is shown a feedback shift register 1, which is applied in any way suitable for that purpose to a portable card, not shown for simplicity's sake, such as a chip card, calling card and the like, having an input 2 and an output 3.

[0028] The feedback shift register 1 comprises a shift register 1a, as well as a feedback function, which in this case consists of a linear function 1b and a non-linear function 1c with the latter having an output 3a. Such a feedback shift register, due to its relatively low costs, is eligible for being applied to, e.g., calling cards and the like. Through the non-linear function, each bit depends on each number of key bits.

[0029] Shift registers are generally known and their operation will therefore not be described in detail. The shift register 1a consists of a series of bits. The length of a shift register is expressed in bits; in the event of a length of n bits, it is called an n-bit shift register.

[0030] Each time a bit is required, all bits in the shift register are shifted 1 bit to the right. The new left bit is calculated as a function of the bits remaining in the register and the input.

[0031] The output of the shift register is 1 bit, often the least significant bit. The period of a shift register is the length of the output series before repetition starts.

[0032] Data is loaded by way of the input 2; the key is loaded, and results are produced by way of the output 3 or, if so desired, 3a. In a similar situation, however, there may be carried out an attack on the secret key used by way of DPA, based on power variations of the system in the event of computations via statistical analysis of "leak data" and error-correcting techniques.

[0033] In this connection, it should be noted that, from a security viewpoint, it is desirable to load the key and the data non-linearly into the shift register. It has become apparent, however, that in the event of calculations, non-linearly loading the key and the data into the shift register increases the chance of deriving the secret key used through statistical analysis of the power consumption.

[0034] In FIG. 2 and FIG. 3, the same reference numerals as used in FIG. 1 refer to the same components.

[0035] FIG. 2 now shows an advantageous embodiment of the invention, the key first being loaded into the shift register, subsequently data being loaded, at least initially, exclusively using the linear-feedback function, and then clocking (e.g., 100 times or more) of the shift register taking place. During loading the data and, if so desired, the subsequent clocking on, the non-linear function of the shift register is deactivated until the shift

register has been sufficiently clocked. Then, the non-linear function is switched once again.

[0036] In doing so, the linear-feedback function 1b continues to be active.

[0037] Deactivating and activating, as the case may be, the non-linear function 1c may take place in any way suitable for that purpose, e.g., using switches.

[0038] The shift register 1a is advantageously clocked so many times that the contents of all elements of the shift register depends on a large portion of the bits of the key.

[0039] In another advantageous embodiment, after loading the key, the shift register is first clocked until the contents of all elements of the shift register depend on a large portion of the bits of the key. Only after this clocking, the data in the shift register 1a is permitted to be loaded and non-linear operations on the contents of the shift register are also permitted to be effected.

[0040] Clocking takes place in any way known to those skilled in the art and will therefore not be explained in further detail.

[0041] For completeness' sake, it should be noted that DPA is only capable of being carried out if a non-linear operation of the data with the key takes place. Since, in addition, the effort required for DPA rises exponentially with the number of key bits on which the bits in the shift register depend, it is achieved in this manner that, in the

event of sufficient interim clocking of the shift register 1a, applying DPA does not result in short-term success.

[0042] In FIG. 3, there is shown an advantageous variant of the invention, the key having been loaded with fixed contents of the shift register (which may also consist purely of zeros) and clocking the shift register taking place with an active linear and an active non-linear feedback function, but without data being loaded into the shift register during the -clocking period. In doing so, the input of data into the shift register after loading the key is disconnected from the shift register and is reinstated again after a specific -clocking period. Due to the fixed contents of the shift register, it is not permitted to apply any modifications and an unauthorized third party shall not be capable of determining a collection of different values of leak data, such as power consumption, and subject it to statistical analysis in order to retrieve the key.

[0043] In this solution according to the invention, the key may therefore be loaded non-linearly, and deactivating the non-linear feedback function will not be required.

[0044] In another advantageous embodiment of the invention, in the event that the key, after data has been loaded into the shift register, is not loaded with the fixed contents of the shift register, the key is loaded into the shift register using only the linear-feedback function, whereafter subsequent clocking is permitted to take place.

[0045] After the aforementioned description, various modifications of the method according to the invention will become apparent to those skilled in the art.

[0046] Such modifications shall be deemed to fall within the scope of the invention.